

AF. TW

PTO/SB/21 (09-04)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

4

Application Number 09/931,629

Filing Date 08/16/2001

First Named Inventor Steven Dale Goodman

Art Unit 2131

Examiner Name Longbit Chai

Attorney Docket Number RPS9 2001 0046

ENCLOSURES (Check all that apply)

<input type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Petition	<input checked="" type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input type="checkbox"/> Power of Attorney, Revocation	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Change of Correspondence Address	<input checked="" type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Terminal Disclaimer	Return Postcard
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Reply to Missing Parts/Incomplete Application	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53		

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Winstead Sechrest & Minick P.C.		
Signature			
Printed name	Kelly K. Kordzik		
Date	7/26/2005	Reg. No.	36,571

CERTIFICATE OF TRANSMISSION/MAILING

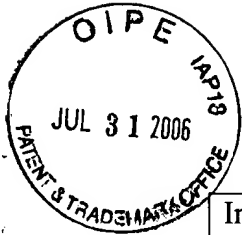
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Danielle Chandler	Date	7/26/2005

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

- 1 -



BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Goodman et al.	:	Before the Examiner:
	:	Chai, Longbit
Serial No.: 09/931,629	:	
	:	Group Art Unit: 2131
Filing Date: August 16, 2001	:	
	:	
Title: FLASH UPDATE USING A TRUSTED PLATFORM MODULE	:	Lenovo (United States) Inc.
	:	ZHHA/B675/B424
	:	P.O. 12195
	:	3039 Cornwallis Road
	:	Research Triangle Park, NC 27709

Mail Stop Appeal Brief - Patents
 Commissioner for Patents
 P.O. Box 1450
 Alexandria, VA 22313-1450

REPLY BRIEF

In response to the Examiner's Answer having a mailing date of May 26, 2006,
 Appellants respond as follows:

The Examiner is asserting that the claims are obvious by combining the
Grawrock reference with the *Alexander* reference. In order to do so, the *prima facie*
 case of obviousness has to show that one skilled in the art at the time the invention
 was made would have been motivated to combine these two references. Appellants

CERTIFICATION UNDER 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with
 sufficient postage as first class mail in an envelope addressed to Mail Stop Appeal Brief - Patents,
 Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on July 26, 2006.

Danielle Chandler

Signature

Danielle Chandler

(Printed name of person certifying)

respectfully assert that one skilled in the art at the time the invention was made would not have been motivated to combine these references as asserted by the Examiner.

Assuming that the *Alexander* reference does describe a process whereby the SMI performs a data verification and then unlocks the flash memory, this is still a software process performed internally within the system. The present invention recites that a BIOS image is used to update the BIOS after it is verified by the TPM, and if the verification is successful, the TPM then unlocks the flash memory to perform the update process. The reason the inventors decided to use a TPM was that it is an external hardware device as opposed to software internal to the system. Using the external TPM hardware to perform the verification and the unlocking of the flash memory, is very secure, since the TPM cannot be spoofed. In contrast, using an SMI to perform such a process is not secure, and in fact, is reliant upon the SMI program that is stored within the BIOS itself. Thus, the present invention provides a greatly superior solution over what is taught in *Alexander*, and not merely an incremental improvement.

So, the question is whether the claimed invention would have been obvious to one skilled in the art looking at the two references. Appellants assert that it would not have, since there is nothing within the *Alexander* reference that suggests using an external piece of hardware such as a TPM to replace any of the software programs described in *Alexander* to perform such an update process, and specifically the SMI. Furthermore, there is nothing within the *Grawrock* reference that suggests using a TPM to perform a BIOS update by first using a TPM to verify the image, and then using a TPM to unlock the flash memory. To combine these references to reject the claims as obvious is relying upon pure hindsight without any objective evidence to show a motivation to combine these references.

As a result of the foregoing, Appellants respectfully assert that the claims are patentable over the cited prior art.

RPS920010046 (44458-P015US)

PATENT

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Appellants

By: 

Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2851

Austin_1\319145\1
44458-P015US 7/26/2006